Texas Department of Information Resources
CYBER SECURITY TIPS
Monthly Newsletter
Office of the Chief Information Security Officer
February 2008 | Volume 2, Issue 2

SECURING A WIRELESS NETWORK

IS A WIRELESS NETWORK SECURE?

Wireless networks are not as secure as the traditional *wired* networks, but you can still minimize the risk to your wireless network (at home and at work) by following the tips listed below.

HOW DOES IT WORK?

The standard configuration for a wireless network requires two components: a Wireless Access Point (WAP) and a computer with a wireless network adaptor. Properly configuring a wireless device can be challenging, and the steps can vary depending on the manufacturer. If you do not feel comfortable doing it yourself, be sure that whomever is configuring the wireless network follows these best practices.

WIRELESS ACCESS POINT

The WAP connects to your high speed Internet connection or your internal network. This is the foundation for building a wireless network. It provides the ability to use a computer without being constrained by the distance of a wire. Keep in mind that metal filing cabinets as well as certain building materials, such as bricks and blocks, can interfere or limit the range. Generally, the indoor range for a WAP is approximately 125 feet.

WIRELESS NETWORK ADAPTOR

A wireless network adaptor, used for transmitting and receiving information, is required for each computer you intend to connect to a WAP. When purchasing wireless networking hardware from separate vendors, obtain guarantees that the hardware will conform to defined standards and interoperate properly. The wireless network adaptor is usually built into laptop computers, while it is an add-on component inserted into a USB port on desktop computers.

ENABLE ENCRYPTION

Every wireless network should enable encryption. Encryption scrambles the data in such a way that if your signal is intercepted, the risk of someone being able to eavesdrop or monitor your communications is reduced. There are several standards of encryption common to most WAPs. Wired Equivalency Privacy (WEP) is the older standard. WEP has a number of known security flaws and should be used only if no other method of encryption is available. Set the WEP authentication method to *shared key* instead of *open system*. Under *open system*, the initial sign-on is encrypted but the data is not. Newer wireless access points include Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA2 is the stronger and preferred method of encryption.

CHANGE THE DEFAULT PASSWORD

Change the default password delivered with your WAP. The default passwords used by manufacturers are well known to the hacking community. Use a strong password of at least eight characters including numbers and special characters.

CHANGE SSID NAME

The Service Set Identifier (SSID) is the name of your wireless network. Default SSIDs are well known; they are often the name of the manufacturer and are easy to guess. Change the SSID name to something unique, and be careful not to use a name that freely discloses information. For example, avoid using your family name. Avoid descriptive or functional names as well, such as *Payroll* or *Accounting* since this would advertise an attractive target for an attacker.

TURN OFF SSID BROADCASTING

By turning off SSID Broadcasting, your wireless access point does not advertise its presence. It is similar to having an unlisted telephone number. This is a way to reduce the visibility of your network to others in your neighborhood. The only way to connect to a WAP with SSID Broadcasting turned off is to know the SSID name and password.

USE MAC FILTERING ON YOUR WAP

The MAC (Media Access Control) address is the unique ID assigned to your computer's network interface card. It is referred to as the computer's *physical address*. Enabling MAC filtering on your WAP allows you to designate and restrict which computers can connect to your WAP. If the computer's address is not listed, a wireless connection cannot be made to the WAP. To look up a MAC address on a Windows computer, select *Start* and *Run*, and then type *cmd*. A new window will open. Then type *ipconfig /all* and press the *Enter* key. A number of attributes will be displayed. The MAC address is identified as the *Physical Address*.

RF INTERFERENCE

Assuming your WAP point functions in the 2.4 GHz range, you may experience Radio Frequency (RF) interference from other 2.4 GHz devices, such as cordless phones, microwaves, and baby monitoring devices. These devices can limit wireless performance. To manage the problem, limit sources of RF interference in proximity to the WAP.

ADDITIONAL RESOURCES

For additional resources regarding wireless networks:

- Wireless Network Tutorial including manufacturer step by step procedures – **spotlight.getnetwise.org/wireless/wifitips**
- Microsoft – **www.microsoft.com/technet/network/wifi/wifisoho.mspx**

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.

For more information on Internet security, please visit the SecureTexas website – **www.dir.state.tx.us/securetexas**. SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by: MS-ISAC www.msisac.org

Powered by: US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM www.us-cert.gov

Distributed by: DIR Secure Texas www.dir.state.tx.us/securetexas